WHAT IS CLAIMED IS:

1. A method of encrypting information, comprising:

generating a first collection and a second collection of encryption bits in a key supply device;

supplying said first collection of encryption bits to a key storage module;

storing said first collection of encryption bits in a memory of said key storage module;

transporting said key storage module to a data production device;

connecting said key storage module to said data production device;

supplying said first collection of encryption bits from said module to said data production device;

deleting said first collection of encryption bits from said memory of said key storage module; and

encrypting data produced by said data production device using said first collection of encryption bits.

2. The method of claim 1, further comprising:

transporting said key storage module to said key supply device;

connecting said key storage module to said key supply device;

supplying said second collection of encryption bits from said key supply device to said key storage module; and

storing said second collection of encryption bits in the memory of the key storage module.

3. The method of claim 2, further comprising:

transporting said key storage module to the data production device;

connecting said key storage module to the data production device;

supplying the second collection of encryption bits from said module to said data production device;

deleting said second collection of encryption bits from the memory of said key storage module; and

encrypting data produced by said data production device using said second collection of encryption bits.

4. The method of claim 1, further comprising:

supplying power from said data production device to said key storage module after said key storage module is connected with said data production device.

5. The method of claim 2, further comprising:

supplying power from said key supply device to said key storage module after said key storage module is connected with said key supply device.

6. The method of claim 1, further comprising:

storing said encrypted data in a memory of said data production device.

7. The method of claim 1, wherein said data production device comprises a communication device.

8. The method of claim 7, further comprising:

transmitting said encrypted data from said communication device to another communication device.

9. A method of encrypting information, comprising:

retrieving a quantity of encryption bits from a memory of a key storage module connected to a port of a communication device, wherein said retrieval depletes a total amount of encryption bits stored in the key storage module; and

encrypting data transmitted from said communication device using said quantity of encryption bits.

10. The method of claim 9, further comprising:

determining whether said retrieval depletes said stored encryption bits below a predetermined amount.

11. The method of claim 10, further comprising:

signaling an encryption bit insufficiency condition when said retrieval depletes said stored encryption bits below said predetermined amount.

12. The method of claim 10, further comprising:

receiving a second quantity of encryption bits from a key supply device based on said determination.

13. The method of claim 12, further comprising:

storing said second quantity of encryption bits in said memory of said key storage module, wherein said second quantity of encryption bits replenishes a total amount of encryption bits stored in said key storage module.

14. A system for encrypting information, comprising:

a key storage module configured to:

store encryption bits in a memory of said key storage module; and

a communication device configured to:

retrieve a quantity of encryption bits from said memory of said key storage module, wherein said retrieval depletes a total amount of encryption bits stored in the key storage module, and

encrypt data transmitted from said communication device using said quantity of encryption bits.

15. The system of claim 14, wherein said key storage module if further configured to:

determine whether said retrieval depletes said stored encryption bits below a specified amount.

16. The system of claim 15, wherein said key storage module if further configured to:

signal an encryption bit insufficiency condition when said retrieval depletes said stored encryption bits below said specified amount.

17. The system of claim 15, wherein said key storage module is further configured to:

receive a second quantity of encryption bits from a key supply device based on said determination.

18. The system of claim 17, wherein said key storage module is further configured to:

store said second quantity of encryption bits in said memory, wherein said second quantity of encryption bits replenishes a total amount of encryption bits stored in said key storage module.

19. A system for encrypting information, comprising:

means for storing a total amount of encryption bits in a memory;

means for retrieving a quantity of encryption bits from said memory, wherein said retrieval depletes the total amount of encryption bits stored in the memory; and

means for encrypting data transmitted from said system using said quantity of encryption bits.

20. A computer-readable medium containing instructions for controlling at least one processor to perform a method of encrypting information at a communication device, the method comprising:

retrieving a quantity of encryption bits from a memory of a key storage module connected to a port of said communication device, wherein said retrieval depletes a total amount of encryption bits stored in the key storage module, and

encrypting data transmitted from said communication device using said quantity of encryption bits.